

Presented to the Court by the foreman of the
Grand Jury in open Court, in the presence
of the Grand Jury and FILED in the U.S.
DISTRICT COURT at Seattle, Washington
January 12, 2022

RAVI SUBRAMANIAN, Clerk

By Sofia Kattar Deputy

Judge Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PAIGE A. THOMPSON,

Defendant.

NO. CR19-159 RSL

**SECOND SUPERSEDING
INDICTMENT**

The Grand Jury charges that:

COUNT 1
(Wire Fraud)

1. Beginning in or before March 2019, and continuing until on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, with the intent to defraud, devised and intended to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises.

A. *Background*

2. The "Cloud Computing Company" is a company that provides cloud-computing services to individuals, companies, and governments. Cloud computing is the practice of using a network of remote servers hosted on the Internet, commonly referred to as "the cloud," rather than a local computer or server, to store, manage, and process

1 data. The Cloud Computing Company provides services through server farms that are
2 located throughout the world and maintained by the Cloud Computing Company.

3 3. Capital One Financial Corporation (“Capital One”) is a bank holding
4 company that offers credit cards and other services to customers throughout the United
5 States. Capital One supports its services, in part, by renting or contracting for computer
6 servers from the Cloud Computing Company. The servers on which Capital One stores
7 credit card application and other information generally are located in states other than the
8 State of Washington, and they store information regarding customers, and support
9 services, in multiple states. Deposits of Capital One are insured by the Federal Deposit
10 Insurance Corporation.

11 4. Victim 2 is a state agency of a state that is not the State of Washington.
12 Victim 2 supports its services, in part, by renting or contracting for computer servers
13 from the Cloud Computing Company.

14 5. Victim 3 is a telecommunications conglomerate located outside the United
15 States that provides services predominantly to customers in Europe, Asia, Africa, and
16 Oceania. Victim 3 supports its services, in part, by renting or contracting for computer
17 servers from the Cloud Computing Company.

18 6. Victim 4 is a public research university located outside the State of
19 Washington. Victim 4 supports its services, in part, by renting or contracting for
20 computer servers from the Cloud Computing Company.

21 7. Victim 5 is a technology company that specializes in digital rights
22 management. Victim 5 supports its services, in part, by renting or contracting for
23 computer servers from the Cloud Computing Company.

24 8. Victim 6 is a technology company that provides data and threat protection
25 services. Victim 6 supports its services, in part, by renting or contracting for computer
26 servers from the Cloud Computing Company.

27 9. Victim 7 is a technology company that provides interaction-management
28 solutions for customer interactions in call centers and other environments. Victim 7

1 supports its services, in part, by renting or contracting for computer servers from the
2 Cloud Computing Company.

3 10. Victim 8 is a technology company that provides higher education learning
4 technology to educational institutions and other clients. Victim 8 supports its services, in
5 part, by renting or contracting for computer servers from the Cloud Computing Company

6 *B. The Essence of the Scheme and Artifice*

7 11. The object of the scheme was to exploit the fact that certain customers of
8 the Cloud Computing Company had misconfigured web application firewalls on the
9 servers that they rented or contracted from the Cloud Computing Company. The object
10 was to use that misconfiguration to obtain credentials for accounts and roles of those
11 customers that had permission to view and copy data stored by the customers on Cloud
12 Computing Company servers, as well as permission to perform other functions. The
13 object then was to use the stolen credentials to access and copy other data stored by the
14 customers on Cloud Computing Company servers, including data containing valuable
15 personal identifying information. The object was also to use the stolen credentials in
16 other ways for PAIGE A. THOMPSON's own benefit, including by using Cloud
17 Computing Company servers to mine cryptocurrency and thereby obtain something of
18 value.

19 *C. The Manner and Means of the Scheme and Artifice*

20 12. It was part of the scheme and artifice that PAIGE A. THOMPSON used,
21 and created, scanners that allowed her to scan the public-facing portion of servers rented
22 or contracted by customers from the Cloud Computing Company, and to identify servers
23 for which web application firewall misconfigurations permitted commands sent from
24 outside the servers to reach and be executed by the servers.

25 13. It was further part of the scheme and artifice that PAIGE A. THOMPSON
26 transmitted commands to the misconfigured servers that obtained the security credentials
27 for particular accounts and roles belonging to the customers with the misconfigured
28 servers.

1 14. It was further part of the scheme and artifice that PAIGE A. THOMPSON
2 used the accounts and roles for which she had obtained security credentials to obtain lists
3 or directories of folders, or buckets, of data in the Cloud Computing Company
4 customers' storage space at the Cloud Computing Company.

5 15. It was further part of the scheme and artifice that PAIGE A. THOMPSON
6 used the accounts and roles for which she had obtained security credentials to copy data,
7 from folders or buckets of data in the Cloud Computing Company customers' storage
8 space at the Cloud Computing Company for which the accounts and roles had requisite
9 permissions, to a server that PAIGE A. THOMPSON maintained at her own residence.

10 16. It was further part of the scheme and artifice that, in taking these steps,
11 PAIGE A. THOMPSON implicitly represented that commands to copy data that she sent
12 using the accounts and roles for which she had obtained security credentials were
13 legitimate commands sent by users with permission to send such commands, rather than
14 commands sent by a person who had stolen the security credentials and who lacked
15 authority to use the accounts and roles and send the commands.

16 17. It was further part of the scheme and artifice that, in executing the scheme
17 and artifice, PAIGE A. THOMPSON used virtual private networks ("VPNs"), including a
18 VPN offered by the company IPredator, to conceal PAIGE A. THOMPSON's location
19 and identity from the Cloud Computing Company and from victim companies.

20 18. It was further part of the scheme and artifice that, in executing the scheme
21 and artifice, PAIGE A. THOMPSON used The Onion Router ("TOR") to conceal PAIGE
22 A. THOMPSON's location and identity from the Cloud Computing Company and from
23 victim companies.

24 19. It was further part of the scheme and artifice that PAIGE A. THOMPSON
25 copied data to her own server from servers rented or contracted by Capital One from the
26 Cloud Computing Company, including data that contained information, including
27 personal identifying information, from approximately 100,000,000 customers who had
28 applied for credit cards from Capital One.

20. It was further part of the scheme and artifice that PAIGE A. THOMPSON copied and stole data from more than 30 different entities, including Capital One, Victim 2, Victim 3, Victim 4, Victim 5, Victim 6, Victim 7, and Victim 8 that had contracted or rented servers from the Cloud Computing Company.

21. It was further part of the scheme and artifice that PAIGE A. THOMPSON used accounts and roles for which she had obtained security credentials to place programs on certain victims' servers to "mine" cryptocurrency for her own benefit using stolen computing power, a practice often referred to as "cryptojacking." (Cryptocurrency mining is the process by which cryptocurrency transactions are verified and added to the public ledger, *i.e.*, the blockchain. Persons who verify blocks of legitimate transactions, often referred to as "miners," are rewarded with an amount of that cryptocurrency. Successful mining operations consume large amounts of computing power and hardware.) PAIGE A. THOMPSON also used the accounts and roles for which she had obtained security credentials to delete the code, logs, and other records of the cryptocurrency mining software and activity.

22. It was further part of the scheme and artifice that, in placing cryptocurrency mining software on victim servers, and deleting the code, logs, and other records from those servers, PAIGE A. THOMPSON implicitly represented that commands that she issued using the accounts and roles for which she had obtained security credentials were legitimate commands sent by users with permission to send such commands, rather than commands sent by a person who had stolen the security credentials and who lacked authority to use the accounts and roles and send the commands.

C. Execution

23. On or about March 22, 2019, at Seattle, in the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, for the purpose of executing the scheme and artifice described above, caused to be transmitted by means of wire communication in interstate commerce, from her computer in Seattle to a computer outside the State of Washington, writings, signs, signals, pictures, and sounds, that is, a

1 command to copy data belonging to Capital One from servers, rented and contracted by
2 Capital One from the Cloud Computing Company, to a server belonging to PAIGE A.
3 THOMPSON in Seattle.

4 All in violation of Title 18, United States Code, Section 1343.

5
6 **COUNT 2**
7 **(Computer Fraud and Abuse)**

8 24. The allegations set forth in Paragraphs 1-23 of this Second Superseding
9 Indictment are realleged and incorporated into this Count, as if fully set forth herein.

10 25. Between on or about March 12, 2019, and on or about July 17, 2019, at
11 Seattle, within the Western District of Washington, and elsewhere, PAIGE A.
12 THOMPSON intentionally accessed a computer without authorization, to wit, a computer
13 containing information belonging to Capital One Financial Corporation, and thereby
14 obtained information contained in a financial record of a financial institution and of a
15 card issuer as defined in Section 1602 of Title 15, and information from a protected
16 computer, and the value of the information obtained exceeded \$5,000.

17 All in violation of Title 18, United States Code, Section 1030(a)(2)(A) and (C),
18 and (c)(2)(A) and (B)(iii).

19
20 **COUNTS 3 -5**
21 **(Computer Fraud and Abuse)**

22 26. The allegations set forth in Paragraphs 1-23 of this Second Superseding
23 Indictment are realleged and incorporated into these Counts, as if fully set forth herein.

24 27. On or about the dates below, at Seattle, within the Western District of
25 Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer
26 without authorization, to wit, computers containing information belonging to the entities
27 identified below, and thereby obtained information from a protected computer, and the
28 value of the information obtained exceeded \$5,000.

<u>Count</u>	<u>Date</u>	<u>Entity</u>
3	April 5, 2019	Victim 3
4	March 7, 2019	Victim 5
5	March 12, 2019	Victim 7

All in violation of Title 18, United States Code, Section 1030(a)(2)(C), and (c)(2)(A) and (B)(iii).

COUNTS 6-7
(Computer Fraud and Abuse)

28. The allegations set forth in Paragraphs 1-23 of this Second Superseding Indictment are realleged and incorporated into these Counts, as if fully set forth herein.

29. On or about the dates below, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, computers containing information belonging to the entities identified below, and thereby obtained information from a protected computer.

<u>Count</u>	<u>Date</u>	<u>Entity</u>
6	March 5, 2019	Victim 6
7	March 28, 2019	Victim 8

All in violation of Title 18, United States Code, Section 1030(a)(2)(C), and (c)(2)(A).

COUNT 8
(Computer Fraud and Abuse)

30. The allegations set forth in Paragraphs 1-23 of this Second Superseding Indictment are realleged and incorporated into this Count, as if fully set forth herein.

31. Beginning on or before March 10, 2019, and continuing until on or after August 5, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, knowingly caused the transmission of a program, information, code, and command, that is a program, code, and commands designed to perform cryptocurrency mining and to delete the code, logs, and other records of the cryptocurrency mining software and activity and, as a result of such conduct, intentionally caused damage without authorization to protected computers rented and contracted by Victim 7, Victim 8, and other victims, from the Cloud Computing Company, and the offense caused loss to one or more persons, that is, Victim 7, Victim 8, other victims, and the Cloud Computing Company, during a one-year period, including loss from a related course of conduct, aggregating at least \$5,000 in value.

All in violation of Title 18, U.S.C. Section 1030(a)(5)(A) and (c)(4)(B)(i).

COUNT 9
(Access Device Fraud)

32. The allegations set forth in Paragraphs 1-23 of this Second Superseding Indictment are realleged and incorporated into this Count, as if fully set forth herein.

33. Beginning on or about March 12, 2019, and continuing until on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, knowingly and with intent to defraud, possessed and attempted to possess counterfeit and unauthorized access devices, said possession affecting interstate and foreign commerce, in that PAIGE A. THOMPSON possessed and attempted to use personal identifying information (PII), including more than 15 Social Security Numbers and more than 15 bank account numbers, stolen during the conduct described in Count 1, to create counterfeit and unauthorized credit and debit cards to be used to conduct transactions in interstate and foreign commerce.

All in violation of Title 18, United States Code, Section 1029(a)(3), (b)(1) and (c)(1)(a)(i).

COUNT 10
(Aggravated Identity Theft)

34. The allegations set forth in Paragraphs 1-23 of this Second Superseding Indictment are realleged and incorporated into this Count, as if fully set forth herein.

35. Beginning on or about March 12, 2019, and continuing until on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, knowingly possessed, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit Wire Fraud, including as charged in Count 1, and Access Device Fraud, as charged in Count 9, knowing that the means of identification belonged to another actual person, to wit, the names and other personal identifying information (PII) of millions of people, including J.B., stolen during the conduct described in Count 1.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

ASSET FORFEITURE ALLEGATION
(COUNT 1)

The allegations contained in Count 1 of this Second Superseding Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c). Upon conviction of the offense charged in Count 1, the defendant, PAIGE A. THOMPSON, shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offense, including but not limited to a sum of money representing the proceeds the defendant obtained from the offense.

//

//

\\

(COUNTS 2-8)

The allegations contained in Counts 2 through 8 of this Second Superseding Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i). Upon conviction of an offense charged in Counts 2 through 8, the defendant, PAIGE A. THOMPSON, shall forfeit to the United States any property constituting, or derived from, proceeds the defendant obtained, directly or indirectly, as the result of such offense, and shall also forfeit the defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense, including but not limited to a sum of money representing the proceeds the defendant obtained from the offense.

(COUNT 9)

The allegations contained in Count 9 of this Second Superseding Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1029(c)(1)(C). Upon conviction of the offense charged in Count 9, the defendant, PAIGE A. THOMPSON, shall forfeit to the United States any property constituting, or derived from, proceeds the defendant obtained, directly or indirectly, as the result of such offense, and shall also forfeit the defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense, including but not limited to a judgment for a sum of money representing the proceeds the defendant obtained from the offense.

(Substitute Assets)

If any of the above-described forfeitable property, as a result of any act or omission of the defendant,

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;

- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

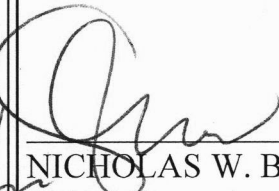
it is the intent of the United States to seek the forfeiture of any other property of the defendant, up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, Section 853(p).

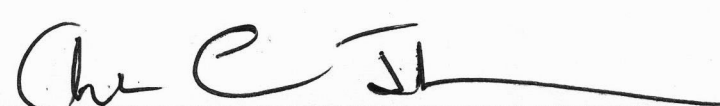
A TRUE BILL:

DATED: 12 January 2022

*Signature of foreperson redacted
pursuant to the policy of the Judicial
Conference of the United States*

FOREPERSON


NICHOLAS W. BROWN
United States Attorney


ANDREW C. FRIEDMAN
Assistant United States Attorney


JESSICA M. MANCA
Assistant United States Attorney